Commonwealth of Massachusetts
Executive Office of Technology Services and Security (EOTSS)
Enterprise Security Office

Secure System and Software Life Cycle Management Standard

Document Name: Secure System and Software Life Cycle Management

Document ID: IS.014

Effective Date: October 15th, 2018

Last Revised Date: October 4th, 2018

Table of contents

1 PURPOSE

1.1. This ***standard*** establishes requirements for identifying controls that shall be incorporated in system and software planning, design, building, testing and implementation, including:

- Information security activities that shall occur during the system and software development life cycle.
- Required controls for supporting system or software development processes such as segregation of environments, prevention and/or protection of ***confidential*** production data in test environments.
- The use of version control for software development.
- Requirements for security hardening when building and configuring systems and applications.

2 AUTHORITY

2.1. M.G.L. Ch. 7d provides that "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3 SCOPE

3.1. This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Department including all executive offices, and all boards, commissions, agencies, departments, divisions, councils, and bureaus. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, such as mass.gov, must agree to comply with this document as a condition of use. Executive Department agencies and offices are required to implement procedures that ensure their ***personnel*** comply with the requirements herein to safeguard information.

4 RESPONSIBILITY

4.1. The Enterprise Security Office is responsible for the development and ongoing maintenance of this ***standard***.

4.2. The Enterprise Security Office is responsible for compliance with this ***standard*** and may enlist other departments in the maintaining and monitoring compliance with this ***standard***.

4.3. Any inquiries or comments regarding this ***standard*** shall be submitted to the Enterprise Security Office by sending an email to EOTSS-DL-Security Office.

4.4. Additional ***information*** regarding this ***standard*** and its related standards may be found at https://www.mass.gov/cybersecurity/policies.

5 COMPLIANCE

5.1. Compliance with this document is mandatory for the Executive Department including all executive offices, and all boards, commissions, agencies, departments, divisions, councils, and bureaus. Violations are subject to disciplinary action in accordance to applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

Exceptions to any part of this document must be requested via email to the GRC Team (ITD-DL-Mass IT - Compliance). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the Commonwealth CISO.

6 STANDARD STATEMENTS

6.1. Security in System and Software Life Cycle

Commonwealth Offices and Agencies must define and oversee a process for addressing security risks throughout the systems development and acquisition life cycles. The agencies must follow a risk-based approach in determining the appropriate level of scrutiny based on the criticality or sensitivity of the system under consideration (see *Information Security Risk Management Standard).*

Security considerations shall be included in the plan, design, build, test and implementation phases of the system and software life cycle.

6.1.1. Plan and scope

6.1.1.1. Initial risk analysis

At the earliest opportunity during the design and development phase, a high-level risk assessment shall be performed by the ***Information Owner*** or designee, with support from the Commonwealth agency's information security ***personnel***, for all significant changes where security is applicable (e.g., new software applications, new software features, introduction of new system and software architecture or a significant modification to existing software application features or existing architecture). See *Information Security Risk Management Standard*. This initial risk assessment should determine whether or not the proposed system or software can operate within the agency's risk profile and identify the initial set of key controls that should be implemented to mitigate any major concerns.

6.1.1.2. Security requirements definition

Based on the initial risk assessment, security-related requirements for the proposed system and/or software shall be identified, validated and incorporated into the design and approved by the ***Information Owner***. Leading security standards shall be used as a reference, such as NIST, OWASP Top 10 and CIS, to provide a comprehensive list of initial requirements for consideration. The security requirements shall be refined and supplemented throughout the systems' or software's life cycle based on follow-on detailed risk assessments.

6.1.2. Design

To ensure that security is incorporated in the system and software life cycle, the system design shall include a "security-as-a-design" objective, and any security exceptions shall be identified by the ***Information Owner*** or ***Information Custodian***.

6.1.2.1. Security design

The ***Information Owner*** and ***Information Custodian*** shall address all high-risk security-related requirements identified during project planning. In addressing these requirements, the following will need to be performed:

6.1.2.1.1 Architecture: Develop design specification and/or security architecture that describes the approach to protecting the confidentiality, integrity and availability of the system.

6.1.2.1.2 Test plans: Test plans shall be in place for validating security testing requirements. The following tests must be performed as applicable.

6.1.2.1.2.1 Threat assessments based on functional requirements

6.1.2.1.2.2 Classification of the data involved

6.1.2.1.2.3 Security requirements gathering and documentation

6.1.2.1.2.4 System design reviews for security

6.1.2.1.2.5 Secure code reviews

6.1.2.1.2.6 Penetration testing

6.1.2.1.2.7 Vulnerability scanning

6.1.2.1.2.8 Host and/or network configuration reviews

6.1.2.1.2.9 Third-party security reviews (design reviews, code reviews, testing, etc.)

6.1.2.1.3 Security design review: Security ***personnel*** shall review the security design for all high-risk security requirements when conducting design reviews prior to build, test and implementation.

6.1.3. Build

Depending on the methodology in use (e.g., waterfall, agile, scrum), security tollgates must be incorporated to ensure secure development.

6.1.4. Test

To ensure and validate that security is incorporated in the system and software life cycle, the following testing is required:

6.1.4.1. Identification and testing of security controls.

Information Owners and ***Information Custodians*** shall test security requirements prior to implementation and use. For software, the following shall be performed:

6.1.4.1.1. Automated source code scanning (static analysis) of all supported code should be performed using a Commonwealth-approved code analysis tool.

6.1.4.1.2. Manual source code analysis should be performed on all ***information system*** source code during testing and prior to deployment.

6.1.4.2. Documentation of change

Any changes to systems and software shall be approved in line with change and release management procedures. Change records shall be made available to security ***personnel*** for review when required.

6.1.5. Implementation

To ensure that security is incorporated in the system and software life cycle, the implementation shall include processes for validation and change control.

6.1.5.1. Validation

Information Owners and ***Information Custodians*** shall ensure that new or significantly changed systems and software applications are released to the production environment only after a pre-implementation security risk assessment and information security issues have been addressed.

6.1.5.2. Change control

Changes related to Commonwealth ***information systems*** and software shall be approved by the respective Change Advisory Board (s*ee Change Management in the Operations Management Standard*) prior to release to production environments (e.g., such as the completion of successful test simulations and resolution of identified issues where applicable).

6.1.5.2.1. Ensure appropriate security controls are in place before approving the change in level for the code.

6.1.5.2.2. Changes that alter the security controls in place at the application, system or network level shall be reviewed prior to release to production.

6.1.5.2.3. All source code and configurations shall be checked into an approved code repository.

6.1.6. Maintenance

Commonwealth Offices and Agencies must ensure that ***Information Owners*** coordinate with Security Officers and the Enterprise Security Office to deploy security patches/updates in a timely fashion to resolve vulnerabilities while ensuring the full functionality of the information system (see *Vulnerability and Patch Management Standard*).

6.1.7. Decommissioning

Prior to decommissioning, the ***Information Owner*** shall formalize plans describing the processes to securely remove, archive or protect sensitive data from the systems to be decommissioned (see *Information Disposal in the Asset Management Standard*).

6.2. Security in SDLC Support Processes

Commonwealth Offices and Agencies must ensure that controls shall be implemented to ensure that the resources, materials and procedures used in the development process are managed to minimize the introduction of security vulnerabilities.

6.2.1 Control application software

The following is required for maintaining application software:

6.2.1.1 Change control processes

All changes to system components must follow the change management process (see IS.012 *Operations Management Standard*).

6.2.1.2 Segregation of environments

Development, test and production environments shall be separated to reduce the risks of unauthorized access or changes to production systems and code repositories. The following rules shall be adhered to:

6.2.1.2.1 Rules for the transfer of software from development to production status shall be logged through a formal recordkeeping system (see IS.012 *Operations Management Standard*).

6.2.1.2.2 Development, test and production software shall run on different systems or computer processors.

6.2.1.2.3 Access controls must be used to enforce access to the development, test and production environments.

6.2.1.2.4 Test environments must emulate the operating system environment as closely as possible.

6.2.1.2.5 Confidential production data should not be copied into the test environment.

6.2.1.2.6 Test data must be removed from systems prior to going live in the production environment.

6.2.1.3 Secure coding practice

Applications shall be developed using secure coding practices to prevent common coding vulnerabilities in software development processes (e.g., OWASP Top 10) to include, but not limited to, the following:

6.2.1.3.1 Injection flaws (e.g., SQL injection, OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws)

6.2.1.3.2 Broken authentication and session management

6.2.1.3.3 Cross-site scripting (XSS)

6.2.1.3.4 Broken access control (e.g., insecure direct object references, failure to restrict URL access and directory traversal)

6.2.1.3.5 Security misconfiguration

6.2.1.3.6 Sensitive data exposure

6.2.1.3.7 Insufficient attack protection (i.e., ability to detect, prevent and respond to both manual and automated attacks)

6.2.1.3.8 Cross-site request forgery (CSRF)

6.2.1.3.9 Using Components with known vulnerabilities (e.g., libraries, software modules)

6.2.1.3.10 Unprotected APIs (e.g., JavaScript in the browser and mobile apps that connect to an API of some kind (SOAP/XML, REST/JSON, RPC, GWT))

6.2.1.3.11 Others, including buffer overflow, insecure cryptographic storage, improper error handling

6.2.1.4 Custom application accounts, user IDs and passwords

Default or custom application accounts, user IDs and passwords shall be removed before systems are moved into production (see *User Access Management in the Access Management Standard).*

6.2.1.5 Release management process

Releasing new systems and application software to the production environment shall follow a defined process that ensures the integrity and accountability for all of the components released. Systems and applications shall not be released to the production environment until use case testing is completed and recorded in source code or configuration change repositories.

6.2.1.6 Vendor software maintenance

Vendor-supplied software (e.g., product upgrades, updates and patches; software developed by the third party) shall be updated and maintained to ensure reduced risk of security vulnerabilities. Change control procedures shall be documented according to the change and release management procedures.

6.2.2 Protection of data integrity

The ***Information Custodian*** is responsible for ensuring system inputs, outputs and processing functions are validated prior to production release in coordination with the development team.

6.2.3 Protection of system test data

The following is required for protecting system test data:

6.2.3.1 Authorization: The use of ***confidential*** production data in a non-production environment is prohibited unless required for a business purpose and explicitly approved by the Information Security Team (see *Release Management in the Operations Management Standard).*

6.2.3.2 Data masking: The use and copying of ***confidential*** production data is prohibited unless masking routines or other protective measures are applied to protect the ***confidential*** production data from unauthorized disclosure.

6.2.3.3 Secure data storage and removal: The storage of ***confidential*** production data used in the development environment shall adhere to the *Information Protection in the Asset Management Standard*. ***Confidential*** production data shall be removed from test systems when it is no longer required.

6.2.4 Protection of application source library

The following is required for protecting application source libraries:

6.2.4.1 Version control: Old versions of production application source libraries shall be archived using version control. Version controlled archives shall contain summary information, including, but not limited to, version numbers and date of last use.

6.2.4.2 Protection from covert channels and malicious code: The creation of covert channels or administrative “back doors” in a system and/or software and its release into the production environment is strictly prohibited. A channel may be considered covert or an administrative “back door” if it allows remote access functionality that was not intended in the software design specifications.

6.3. System Hardening

Commonwealth Offices and Agencies must ensure that operating systems for email, application, web, database, network devices and file servers shall be hardened to protect from exploitation from non-authorized or malicious use. Adherence to hardening standards to harden or secure Commonwealth ***information assets*** prior to deployment into production environments is mandatory.

i. Technical security standards

Technical security standards shall be developed for all critical and high-risk information systems. These standards shall address known security vulnerabilities and must be consistent with industry-accepted system hardening standards.

It is the responsibility of application and platform owners in collaboration with the Enterprise Security Office to develop technical standards for critical and high-risk systems that they own or support.

1. Risk assessment: ***Information Owners*** shall perform a regular risk assessment to determine if existing/planning controls adequately meet the criticality and sensitivity of the ***information asset***. More restrictive controls may be implemented as needed.

2. Review of technical standards: Systems shall be reviewed periodically for compliance with technical standards by ***Information Custodians***, information security ***personnel*** or the appropriate designee to ensure regular compliance:

   a. ***Information Custodians*** are responsible for ensuring and maintaining compliance with technical standards.

   b. Information security teams are responsible for monitoring and measuring compliance with technical standards.

ii. Primary system function

Implement only one primary function per server (or virtual server) to prevent functions that require different security levels from coexisting on the same server (e.g., web servers, database servers, DNS).

iii. Patch management

Apply most up-to-date vendor-supplied security patches or upgrades to correct for known vulnerabilities. Security patches should be deployed in a timely manner and consistent with the patch deployment schedule defined in the *Vulnerability and Patch Management Standard*. Any known vulnerabilities with the OS shall be remediated (or a risk exception must be requested and approved) accordingly before using it to host a server.

iv. Disabling or removing unnecessary services

Disable or remove service, applications and network protocols that are not required when configuring the OS. Minimal OS configurations shall be installed and services, applications and network protocols shall be added as needed for business purposes. Common types of services and applications that should be removed include but are not limited to:

1. File and printer sharing services (e.g., Windows Network Basic Input/Output System [NetBIOS] file and printer sharing, Network File System [NFS], FTP)

2. Wireless networking services

3. Remote control and remote access programs, particularly those that do not strongly encrypt their communications (e.g., Telnet)

4. Directory services (e.g., Lightweight Directory Access Protocol [LDAP], Network Information System [NIS])

5. Web servers and services

6. Unnecessary scripts and drivers

7. Unnecessary subsystems and file systems

8. Email services (e.g., SMTP)

9. Language compilers and libraries

10. System development tools

11. System and network management tools and utilities, including Simple Network Management Protocol (SNMP)

v. Disabling or removing default accounts

Operating system account defaults shall be reviewed and updated by removing or disabling account default configurations (*see Account Management in the Access Management Standard*). Controls for user authentication include but are not limited to:

1. Disable or remove interactive default accounts. For default accounts that need to be retained, restrict access and change the name (where possible) and default password.

2. Disable or remove non-interactive (e.g., system) accounts and their associated passwords.

vi. Configuring system security parameters

System security parameters shall be configured to prevent misuse. System administrators and security resources should be knowledgeable of common security parameter settings for system components. Common system security parameters shall be included in technical security standards and set appropriately on system components.

vii. Full disk encryption

Full disk encryption shall be deployed for operating systems containing ***confidential*** information (see *Endpoint Security in the Asset Management Standard* and *Cryptographic Management Standard*).

viii. Other security hardening requirements

1. Reduce the attack surface presented by systems, platforms and applications comprising the ***information system***. Secure resources according to least privilege.

2. ***Information systems*** that implement or connect to a directory containing non-public information must not permit anonymous binds.

3. ***Information systems*** that integrate with a directory used for authentication, authorization or identity information must connect over a secure connection.

4. File permissions on back-end configuration, system and application files must restrict access to authorized ***personnel*** and these files must not be accessible through the application or other non-administrative services.

5. All servers must be kept in sync with a time synchronization mechanism.

6. All vendor-supplied defaults must be changed to values appropriate to the environment (e.g., default passwords, SNMP permissions and community strings).

7. All services must run in the context of a non-privileged user.

8. Web servers must be configured to support only the HTTP methods required for application operation.

9. Information systems which implement HTML 5 must adhere to the HTML 5 Security Standard.

10. Network services must be configured to not allow low-grade TLS encryption and should adhere to the *Cryptographic Management Standard*.

11. Web servers must be configured to disallow directory listing.

12. Logging of detailed debugging information must be disabled on production systems.

13. Only the current non-debug-release of production code should be installed on production servers; non-production code and backup files must be removed.

14. Web servers must set folder permissions according to least privilege (e.g., disable unnecessary access, execute and write permissions).

7 CONTROL MAPPING

Section	NIST SP800-53 R4 (1)	CIS 20 v6	NIST CSF
6.1 Security in System and Software Lifecycle	PL-7	-	-
	PL-8	CSC 1	ID.AM-3
	SA-13	-	-
	SA-3	-	PR.IP-2
	SA-4	-	PR.IP-2
	AU-10	CSC 6	PR.PT-1
	IA-8	CSC 16	PR.AC-1
	SC-7	CSC 9	PR.AC-5
	SC-8	CSC 13	PR.DS-2
	SC-3	-	-
	RA-3	CSC 4	ID.RA-1
6.2 Security in SDLC Support Processes	AC-3	CSC 5	PR.AC-4
	AC-6	CSC 5	PR.AC-4
	CM-5	CSC 3	PR.IP-1
	CM-9	CSC 3	PR.IP-1
	MA-5	-	PR.MA-1
	SA-Family	-	-
	CM-1	-	ID.GV-1
	CM-3	CSC 3	PR.IP-1
	CM-4	CSC 3	PR.IP-1
	SI-2	CSC 4	ID.RA-1
	IR-9	-	-
	AC-4	CSC 1	ID.AM-3
	SI-Family	-	PR.IP-3
	PE-19	CSC 13	PR.DS-5
6.3 System Hardening	SI-2	CSC 4	ID.RA-1
	SI-3	CSC 8	DE.CM-4
	SI-4	CSC 4	ID.RA-1
	SA-6	-	-
	SI-1	-	ID.GV-1
	SI-6	-	-
	SI-8	-	-

8 RELATED DOCUMENTS

Document	Effective date

9 DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.9	Jim Cusson	10/01/2017	Corrections and formatting.
0.95	Sean Vinck	5/7/2018	Corrections and formatting.
0.97	Andrew Rudder	5/31/2018	Corrections and formatting.
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	06/01/2018	Prepublication review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto

The owner of this document is the Commonwealth CISO (or designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement should be submitted to the document owner.

9.1 Annual Review

This *Secure System and Software Life Cycle Management Standard* should be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.